



Product Component

DEFINITION

<i>Name</i>	CS-MARS – (Cisco Monitoring, Analysis and Response System).
<i>Description</i>	CS-MARS is a hardware and software device which can include single or multiple appliances used to perform network security functions.
<i>Rationale</i>	It offers the ability to centrally monitor network security devices, perform threat management and the ability to mitigate suspect activity to maintain network security compliance.
<i>Benefits</i>	<ul style="list-style-type: none"> • Can be distributed within an agency network based upon segment, group, physical location, etc. • Scalable • Correlates and aggregates logs with events from SNMP supported network devices, security devices and appliances, hosts, applications, and network traffic into a central database. • Uses a customized rule base to reduce false positives. • Cost is not based upon number of devices monitored.

ASSOCIATED TECHNOLOGY AREA

<i>List the name of the associated Technology Area</i>	Intrusion Detections Systems
--	------------------------------

KEYWORDS

<i>List all Keywords</i>	IPS, IDS, detection, security, devices, compliance, anomalies, attacks
--------------------------	--

VENDOR INFORMATION

<i>Vendor Name</i>	Cisco	<i>Website</i>	www.cisco.com
<i>Contact Information</i>			

POTENTIAL COMPLIANCE ORGANIZATIONS/GOVERNMENT BODIES

Standard Organizations

<i>Name</i>		<i>Website</i>	
<i>Contact Information</i>			

Government Bodies			
Name	Sarbanes-Oxley, the Gramm-Leach Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and the Federal Information Security Management Act (FISMA) in the United States, and the EU's Revised Basel Capital Framework (Basel II).	Website	
Contact Information			
COMPONENT REVIEW			
Platform Information			
Hardware Platform Support	No additional hardware is required to install and operate CS-MARS		
Operating System Support	Hardened Linux operating system software.		
Review Aspects			
List Desirable aspects	<ul style="list-style-type: none"> Provides network intelligence to correlate network anomalies and security events Validates incidents Mitigates attacks by taking advantage of existing network and security infrastructure Monitors systems, network, and security operations to aid in compliance 		
List Undesirable aspects	<ul style="list-style-type: none"> Proprietary system No professional training is available Product is in infancy stage May require other Cisco products to be fully implemented 		
ASSOCIATED COMPLIANCE COMPONENTS			
Product			
List the Product-specific Compliance Component Names	None		
Configuration Links			
List the Configuration-specific Compliance Component Names	None		
COMPONENT CLASSIFICATION			
Provide the Classification	<input type="checkbox"/> Emerging <input checked="" type="checkbox"/> Current <input type="checkbox"/> Twilight <input type="checkbox"/> Sunset		

COMPONENT SUB-CLASSIFICATION			
Sub-Classification	Date	Additional Sub-Classification Information	
Technology Watch			
Variance			
Conditional Use			
RATIONALE FOR COMPONENT CLASSIFICATION			
Document the Rationale for Component Classification			
MIGRATION STRATEGY			
Document the Migration Strategy			
IMPACT POSITION STATEMENT			
Document the Position Statement on Impact			
AGENCIES			
List the Agencies Currently Utilizing this Product	DOLIR, OA, OSCA		
CURRENT STATUS			
Provide the Current Status	<input type="checkbox"/> In Development <input type="checkbox"/> Under Review <input checked="" type="checkbox"/> Approved <input type="checkbox"/> Rejected		
AUDIT TRAIL			
Creation Date	06/08/06	Date Accepted / Rejected	06/13/06
Reason for Rejection			
Last Date Reviewed		Last Date Updated	
Reason for Update			